''बेटी बचाओ, बेटी पढ़ाओ''

JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name – Cryptography and Network Security

Session no.: 14

Session Name- Data Encryption Standard Design Principals

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem.**

Lecture starts with- quotations' answer writing

Review of previous Session **– Data Encryption Standard Modes of use**

Topic to be discussed today- Today We will discuss about **DES Design Principals**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic **– Data Encryption Standard**

Data Encryption Standard (DES) Design Principals

Although the standard for DES is public, the design criteria used are classified and have yet to be released. some information is known, and more has been deduced

– L P Brown, "A Proposed Design for an Extended DES", in Computer Security in the Age of Information, W. J. Caelli (ed), North-Holland, pp 9-22, 1989

– L P Brown, J R Seberry, "On the Design of Permutation Boxes in DES Type Cryptosystems", in Advances in Cryptology - Eurocrypt '89, Lecture Notes in Computer Science, vol 434, pp 696-705, J.J. Quisquater, J. Vanderwalle (eds), Springer-Verlag, Berlin, 1990.

– L P Brown and J R Seberry, "Key Scheduling in DES Type Cryptosystems," in Advances in Cryptology - Auscrypt '90, Lecture Notes in Computer Science, vol 453, pp 221-228, J. Seberry, J. Pieprzyk (eds), Springer-Verlag, Berlin, 1990.

will briefly overview the basic results, for more detailed analyses see the above papers

DES S-Box Design Criteria

Each S-box may be considered as four substitution functions

○ these 1-1 functions map inputs 2,3,4,5 onto output bits

○ a particular function is selected by bits 1,6

○ this provides an **autoclave feature**

DES Design Criteria

- there were 12 criteria used, resulting in about 1000
- possible S-Boxes, of which the implementers chose 8
- these criteria are CLASSIFIED SECRET
- however, some of them have become known
- The following are design criterion:

R1: Each row of an S-box is a permutation of 0 to 15

R2: No S-Box is a linear of affine function of the input

R3: Changing one input bit to an S-box results in changing at least two output bits

R4: S(x) and S(x+001100) must differ in at least 2 bits

- The following are said to be caused by

design criteria R5: S(x) [[pi]] S(x+11*ef* 00)
for any choice of *e* and *f*
R6: The S-boxes were chosen to minimize the difference between the number of 1's and 0's in any S-box output when any single input is held constant

R7: The S-boxes chosen require significantly more minterms than a random choice would require Meyer Tables 3-17, 3-18

DES Permutation Tables

- there are 5 Permutations used in DES:

○ IP and IP^(-1) , P, E, PC1, PC2

- their design criteria are CLASSIFIED SECRET

it has been noted that **IP** and **IP^(-1)** and **PC1** serve no cryptological function when DES is used in ECB or CBC modes, since searches may be done in the space generated after they have been applied

- **E, P,** and **PC2** combined with the S-Boxes must supply the required dependence of the output bits on the input bits and key bits (**avalanche** and **completeness** effects)

Ciphertext Dependence on Input and Key

- the role of **P, E,** and **PC2** is distribute the outputs of the S-boxes so that each output bit becomes a function of all the input bits in as few rounds as possible
- Carl Meyer (in Meyer 1978, or Meyer & Matyas 1982) performed this analysis on the current DES design

- Ciphertext dependence on Plaintext

- define **G_(i,j)** a 64*64 array which shows the dependence of output bits X(j) on input bits X(i)

- examine **G_(0,j)** to determine how fast complete dependence is achieved
- to build **G_(0,1)**
  use the
  following
  L(i) = R(i-1)
- R(i) = L(i-1) (+) f(K(i), R(i-1))
- DES P reaches complete dependence after 5 rounds
- []

Ciphertext dependence on Key

- Carl Meyer also performed this analysis
- define **F_(i,j)** a 64*56 array which shows the dependence of output bits X(j) on key bits U(i) (after PC1 is used)
- examine **F_(0,j)** to determine how fast complete dependence is achieved
- DES PC2 reaches complete dependence after 5 rounds

Key Scheduling and PC2

- Key Schedule
  - is a critical component in the design
  - must provide different keys for each round otherwise security may be compromized (see Grossman & Tuckerman 1978)
  - current scheme can result in weak keys which give the same, 2 or 4 keys over the 16 rounds
- Key Schedule and PC-2 Design
  - is performed in two 28-bit independent halves

  - C-side provides keys to S-boxes 1 to 4
  - D-side provides keys to S-boxes 5 to 8
  - the rotations are used to present different bits of the key for selection on successive rounds
  - PC-2 selects key-bits and distributes them over the S-box inputs

Possible Techniques for Improving DES

- multiple enciphering with DES
- extending DES to 128-bit data paths and 112-bit keys
- extending the Key Expansion calculation

Triple DES

- DES variant
- standardised in ANSI X9.17 & ISO 8732 and in PEM for key management
- proposed for general EFT standard by ANSI X9
- backwards compatible with many DES schemes
- uses 2 or 3 keys

  C = DES_(K1) Bbc{(DES^(-1)_(K2)Bbc{(DES_(K1)(P)))

- no known practical attacks
  - brute force search impossible
  - meet-in-the-middle attacks need 2^(56) PC pairs per key
- popular current alternative

Reference-

1. **Book:** William Stallings, "Cryptography & Network Security", Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. What are the designing principals of the DES?

Q2. Explain permutation table in DES?

Q3. Explain the three data encryption standard (3-DES).

Next, we will discuss about IDEA (IPES)

- Academic Day ends with-
  National song 'Vande Mataram'